Strategy Research Project

DOMESTIC INTELLIGENCE AND HOMELAND SECURITY: ARE WE THERE YET?

BY

COLONEL GREGORY D. LAUTNER
United States Army

USAWC CLASS OF 2010

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-02-2010	Strategy Research Project	

4. TITLE AND SUBTITLE

Domestic Intelligence and Homeland Security: Are We There Yet?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Gregory D. Lautner

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Constance Phlipot
Department of National Security and Strategy

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This paper assesses domestic intelligence and its application to homeland security to show that even though tremendous gains have been made the domestic intelligence system faces many problems in its organizational structure, in information sharing, and in intelligence analysis.

To address this topic, this paper will first distinguish the differences between intelligence, law enforcement intelligence, and domestic intelligence to establish a common framework used throughout the paper. This research paper also critically examines current legislation that governs domestic intelligence activities to highlight restrictions on domestic intelligence collection and their associated impact while making recommendations to improve policy. It reviews current organizational processes for intelligence/information gathering and sharing to demonstrate that there are systems in place to share information between localities, states, and the federal government. Lastly, this paper scrutinizes institutional biases to show that even though progress has been made in the intelligence community and other departments and agencies, institutional biases impede organizational integration, cooperation and intelligence/information sharing.

15. SUBJECT TERMS
Domestic Intelligence System, ODNI, IC, Patriot Act, Intelligence Reform and Terrorism Protection Act, Foreign Intelligence and Surveillance Act, DHS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER**
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	40	*(include area code)*

USAWC STRATEGY RESEARCH PROJECT

DOMESTIC INTELLIGENCE AND HOMELAND SECURITY: ARE WE THERE YET?

by

Colonel Gregory D. Lautner
United States Army

Professor Constance Phlipot
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Gregory D. Lautner

TITLE: Domestic Intelligence and Homeland Security: Are We There Yet?

FORMAT: Strategy Research Project

DATE: 1 February 2010 WORD COUNT: 7,976 PAGES: 40

KEY TERMS: Domestic Intelligence System, ODNI, IC, Patriot Act, Intelligence Reform and Terrorism Protection Act, Foreign Intelligence and Surveillance Act, DHS

CLASSIFICATION: Unclassified

This paper assesses domestic intelligence and its application to homeland security to show that even though tremendous gains have been made the domestic intelligence system faces many problems in its organizational structure, in information sharing, and in intelligence analysis.

To address this topic, this paper will first distinguish the differences between intelligence, law enforcement intelligence, and domestic intelligence to establish a common framework used throughout the paper. This research paper also critically examines current legislation that governs domestic intelligence activities to highlight restrictions on domestic intelligence collection and their associated impact while making recommendations to improve policy. It reviews current organizational processes for intelligence/information gathering and sharing to demonstrate that there are systems in place to share information between localities, states, and the federal government. Lastly, this paper scrutinizes institutional biases to show that even though progress has been made in the intelligence community and other departments and agencies,

institutional biases impede organizational integration, cooperation and intelligence/information sharing.

DOMESTIC INTELLIGENCE AND HOMELAND SECURITY: ARE WE THERE YET?

> To kill the Americans and their allies -- civilians and military -- is an individual duty for every Muslim who can do it in any country in which it is possible to do it.
>
> —Osama bin Laden[1]

The tragic events of September 11th, 2001, forever changed our view of homeland security and the way we, as a nation, protect ourselves against future threats. In response to the 9/11 Commission recommendations, the United States government instituted a number of changes. The Department of Homeland Security was created to secure the nation from various threats; the National Counterterrorism Center was established to lead the country's effort in combating terrorism; and the Director of Central Intelligence was replaced by a Director of National Intelligence to head the intelligence community and oversee and direct the National Intelligence Program, while serving as the principal advisor the President.

This paper assesses domestic intelligence and its application to homeland security to show that even though tremendous gains have been made the domestic intelligence system faces many problems in its organizational structure, in information sharing, and in intelligence analysis.

To address this topic, this paper will first distinguish the differences between intelligence, law enforcement intelligence, and domestic intelligence to establish a common framework used throughout the paper. This research paper also critically examines current legislation that governs domestic intelligence activities to highlight restrictions on domestic intelligence collection and their associated impact while making recommendations to improve policy. It reviews current organizational processes for

intelligence/information gathering and sharing to demonstrate that there are systems in place to share information between localities, states, and the federal government. Lastly, this paper scrutinizes institutional biases to show that even though progress has been made in the intelligence community and other departments and agencies, institutional biases impede organizational integration, cooperation and intelligence/information sharing.

Framing the Discussion: Definitions and National Strategies

Debate over the meaning of intelligence and law enforcement intelligence is not new and predates 9/11. However, in the wake 9/11 this debate took on added importance. It also spawned the rise of domestic intelligence and the need to more precisely define homeland security.

Homeland security, according to the *National Strategy for Homeland Security, October 2007*, is "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[2]

Additionally, the difference between intelligence and law enforcement intelligence can best be characterized as information used for "cops and spies," or as Arthur S. Hulnick, professor and 30 year intelligence professional opines, intelligence is used to "string people along," while intelligence in law enforcement is used to "string them up."[3] In essence, the debate is over the "foreign and domestic divide." This will be amplified in subsequent paragraphs.

Intelligence, is defined in *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, as "the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available

information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. "[4]

Next, a survey of literature reveals there is no technical definition of law enforcement intelligence, or police intelligence applicable at the strategic level. However, the research indicates that the intelligence community (IC), Department of Homeland Security (DHS), and scholars agree that intelligence used in law enforcement is used primarily to obtains warrants, and is evidence to gain convictions in criminal cases.

As mentioned earlier the divide between domestic and foreign intelligence is not new. However, the recognition that increased threats inside America originate from foreign entities brings the meaning of these two terms closer together blurring their distinctions.

The term domestic intelligence is a common term used throughout academia and government. However, like law enforcement or police intelligence, there is no formal strategic definition. Although the Department of Defense (DoD) has a definition, it is too narrow. Furthermore, it not only acknowledges intelligence relating to threats to internal security, but the definition also links it to the potential use of troops, and to threats against DoD. The closest statutory definition of domestic intelligence appears in the *Homeland Security Act of 2002*. It defines homeland security "information" as

> any information possessed by a federal, state, or local agency that (a) related to the threat of terrorist activity, (b) relates to the ability to prevent, interdict or disrupt terrorist activity, (c) would improve the identification of investigation of a suspected terrorist or terrorist organization: or (d) would improve the response to a terrorist act.[5]

Furthermore, to close the gap between foreign and domestic intelligence Congress passed the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA). The IRTPA amended the National Security Act of 1947;

> The terms 'national intelligence' and 'intelligence related to 'national security' refer to all intelligence, regardless of source from which derived and including information gathered within or outside the United States that (a) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and (b) that involves – (I) threats to the United States, its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on U.S. notational or homeland security.[6]

These definitions and terms set the backdrop for key elements of the *National Intelligence Strategy* (NIS) and the *National Strategy for Homeland Security*, and the corresponding implementing laws to the strategies.

Even though there is a two year gap between the two strategies they are complimentary, mutually supporting, and interdependent, with four necessary and important provisions.

First, both have similar principles and goals. The 2009 NIS establishes "responsive and incisive understanding of global threats and opportunities, coupled with the agility that brings to bear the Community's capabilities" as guiding principles.[7] It is also forward thinking by setting the Intelligence Community's (IC) priorities, plans, and actions for the next four years, while pointing out areas that require attention and commitment.[8]

In a similar manner, the 2007 *National Strategy for Homeland Security* seeks to "guide, organize, and unify" security efforts at home by focusing the nation on the following goals: prevent and disrupt terrorist attacks, protect the American people –

critical infrastructure – key resources, respond to and recover from incidents that do occur, and continue to strengthen the foundation to ensure our long-term success.[9]

Next, the strategies advocate the whole-of-government approach. In the NIS "the intelligence community supports the whole-of-U.S. Government efforts to protect the homeland…warn of impending attacks…disrupt, dismantle, or defeat their operation."[10] Likewise, in the *National Homeland Security Strategy* "homeland security requires a truly national effort, with shared goals and responsibilities for protecting and defending the Homeland…leverages the unique strengths and capabilities of all levels of government."[11]

Third, the NIS and the *National Strategy for Homeland Security* recognize the attributions and contributions from all echelons of government and the private sector and include them as contributing members of the IC. The NIS dedicates one of its enterprise objectives (EO 2) to "strengthen partnerships."[12] The IC strives to "strengthen existing and establish new partnerships with foreign and domestic, public and private entities."[13] To accomplish this objective the strategy focuses on "building familiarity" or becoming familiar with the capabilities of all partners, including nontraditional members of the IC, and expanding partnerships to guide and improve collaboration and information sharing.

The National Strategy for HS also embraces this notion and is more attuned to the value and contributions from all sectors of society. It is addressed throughout the strategy, but best expressed in its "Shared Responsibility" section. The strategy attributes much of the DHS's success to "the notion that homeland security is a shared responsibility upon a foundation of partnerships…state, local and tribal governments,

which best understand their communities…always play a prominent and frontline role in helping to prevent terrorist attacks."[14] Moreover, as providers of goods and services and owners of 85% of the nations critical infrastructure and business "private and non-profit sector also must be full partners in homeland security."[15]

The fourth and most important element the strategies share is information sharing. The emphasis on information sharing is a direct result of 9/11 and the divide between foreign and domestic intelligence. As mentioned earlier, the IRTPA bridged the gap between the two types of intelligence/information by redefining them. As a result, the strategies dedicate portions toward improving the seamless flow of relevant information vertically and horizontally throughout governance and the private sector.

The NIS' EO 4, *Improve information Integration & Sharing*, endeavors to "radically improve the application of information technology…integration and sharing practices, systems and architectures (both across the IC and with an expanded set of user and partners)."[16] Similarly, *Leveraging instruments of National Power and Influence* in the National Strategy for HS describes the congressionally mandated creation of the Information Sharing Enterprise (ISE). The ISE is "a trusted partnership among all levels of government, the private sector, and our foreign partners to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism…through the appropriate exchange of terrorism."[17] This was later amended to include information relating to weapons of mass destruction.

These definitions and terms, as well as the review of our nation's relevant strategies set the conditions for introducing the implementing legislature that facilitates the collection and gathering of intelligence/information while maintaining a balance with

civil liberties and American values. Legendary spy master, linguist, and ambassador Vernon Walters said it best, “Americans have always had an ambivalent attitude toward intelligence. When they feel threatened, they want a lot of it, and when they don’t, they regard the whole thing as somewhat immoral.”[18]

Legislature

In the aftermath of 9/11, the President and Congress created the Patriot Act of 2001 and the Intelligence Reform and Terrorism Protection Act (IRTPA) of 2004 while making temporary and controversial amendments to the 1978 Foreign Intelligence Surveillance Act (FISA) to prevent future attacks against the homeland of the United States. This section addresses the three most controversial sections of legislature that altered the way the Intelligence and law enforcement communities gather intelligence and information in support of domestic intelligence.

The first provision is **Section 6001 (a*)*** of the IRTPA, commonly referred to as the **“*lone wolf*”** provision. This provision simplifies the “evidentiary showing needed to obtain a Foreign Intelligence and Surveillance Act Court (FISC) order” to collect on “individuals other than U.S. citizens or permanent residents, engaged in international terrorism.”[19] This provision changed the rules regarding the type of individual subject to a FISA search. Surveillance of an individual engaged with terrorism is permissible without evidence linking that person to an “identifiable foreign power or terrorist organization.”[20]

The “Lone Wolf” provision originates from the post 9/11 investigation of the intelligence community. According to numerous reports and investigative summaries the FBI and the CIA had intelligence information regarding the potential for a sensational attack in the U.S. However, a specific target, time, and location were not

known at the time. Moreover, information contained by the FBI and CIA was not shared between the two agencies. Further reporting revealed that an investigation into one of the individuals involved in the attacks had been stifled as a result of perceived limitations under FISA.[21]

In October 2001, the FBI detained Zacarias Moussaoui, a French foreign national who was in the U.S. illegally. Moussaoui was suspected of planning a terrorist attack in the U.S. involving the use of commercial airplanes. The FBI subsequently requested a FISA Court (FISC) order to analyze information on Moussaoui's computer, but later concluded that they did not have enough evidence and probable cause linking Zacarias Moussaoui as an agent to a foreign power required under the existing FISA. The FISA of 2001 applied only to those involved in terrorism on behalf of a foreign power, or as an agent of a foreign power. The law, at that time, did not account for terrorism from non-state actors such as Al Qaida.[22]

These ambiguities were adjusted in the IRTPA of 2004. The provision now "presumes" that individuals, not permanent U.S. residents or citizens, involved with terrorist activities are agents of a foreign power.[23]

Opponents of the Lone Wolf provision argue that Moussaoui's lap top could have been searched under standard criminal warrants and that FISA, if extended, will become a substitute for some of the nation's most important laws. Proponents of extending the provision, on the other hand, claim that the decentralized, compartmentalized, and secret nature of today's evolving terrorism makes proving links to a foreign power difficult, thus justifying the current provision.[24]

The next section under consideration is **Section 206** of the US Patriot Act. This section permits ***"roving" wiretaps*** based on the situation and affords flexibility in the way the target of a FISC is specified.[25] Flexibility is applied to the specificity of the location or facility for electronic surveillance identified under FISA.

Prior to enactment in 2001, electronic surveillance under provision 206 had two limitations. It first required identification of the specific location or facility for surveillance. Next, only known third parties (telecommunication providers, land lords etc.) could be ordered by the government to assist in electronic surveillance. These sources were, and still are, the only means to obtain the requisite surveillance. Additionally, only the FISC could direct telecommunications providers to assist in foreign intelligence collection. Nevertheless, without a known specific location or facility the FISC could not authorize or direct a third party collector to support electronic surveillance.[26]

In addition to the "roving" wiretaps amendment, there were two sub-amendments to section 206. The first was the "other persons" amendment. The law was changed to permit the FISC to order "unspecified" persons to assist the government in electronic surveillance in places or locations unknown at the time. This is based on knowledge that a target would attempt to impede the electronic surveillance. The second amendment requires the FISC be notified within ten days of initiation of electronic surveillance. This includes the necessary facts and circumstances that justify the surveillance, changes from the original FISC order, and changes in location of electronic surveillance.[27]

Those against section 206 argue that roving wire taps collect on those persons not subject to an investigation, thus violating the Fourth Amendment's particularity clause. This clause stipulates that warrants shall "particularly describ[e] the place to be searched."[28] This creates a conundrum between homeland security and civil liberties, as FISA only requires a description of a target and its location, not the specific identification.

The third provision under consideration is **Section 215** of the Patriot Act. Section 215 broadens the types of ***records, documents, and information*** collected and made available to the US Government. It also lowers the standards required prior to issuing a "court order compelling the production of documents."

In 2001, and 2005, Section 215 was amended and expanded from four explicit business categories to "any tangible things." Examples of "tangible things" include, but are not limited to: "library circulation records and patron lists, book sales records and customer lists, firearms sales records, tax return records, educational records, and medical records containing information" indentifying an individual, to name a few.[29]

Standards for ordering the "compelling production" of documents were also reduced. Prior to the Patriot act "specific and articulable facts" were required in the belief that the subject was linked to a foreign power or served as an agent of a foreign power. Under the current amendment the standard for "compelling production" requires "a statement of fact showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence investigation]."[30]

Another component of Section 215 is a nondisclosure and judicial review. These orders include a nondisclosure clause that prohibits the person surrendering the

documents from disclosing involvement in the FISA order. However, communication with others needed to comply with the order is authorized. Consequently, information on others consulted in the execution of the FISA order is required by the FBI.[31]

Judicial reviews of nondisclosure orders occur annually. Petitions are set aside if the FISC determines that disclosure would not "endanger the national security of the United States…interfere with diplomatic relations." [32]

Finally, all three provisions, Section 6001 (a*)* - lone wolf, Section 206 - roving wiretaps, and Section 215 - records, documents, and information were to expire on 31 Dec 05. Instead, they were extended until 31 Dec 09, by the USA Patriot Improvement and Reauthorization Act of 2005. If allowed to expire all three provisions will read as they did on 25 Oct 01. Additionally, the original sunset provision for the lone wolf section and business records section includes grandfather clauses whereby ongoing investigations at expiration will be permitted to continue under the current law.[33]

In December 2009, the 111th Congress convened. On the agenda was a decision to allow the three provisions to sunset on 31 December 09 or extend them until 31 December, 2019. Congress tabled the debate until 28 February 2010.[34] This means that the provisions remain law, as written, until 28 February, or until Congress convenes to decide. It further permits the IC and law enforcement community to continue to collect or gather intelligence/ information under the current provisions of the law.

During this pause, the Administration should convince Congress to extend the provisions through 2019, or make the amendments permanent. The nation has a conglomerate of organizations (ODNI, NCTC, DHS, CIA, FBI, DOD, state/local fusion centers, and private sector) systems, procedures, and oversight (House and Senate

committees, DoJ IG, internal organizational IG's) in place that has proven to be successful in the post 9/11 environment. Although the new and restructured departments and agencies are a work in progress, up to 19 terrorist plots and several domestic cases involving American radicalism that we know of have been thwarted or disrupted over the past nine years. The amended 2001 Patriot Act, IRTP of 2004, and FISA directly attributed to these small victories.

Even though the legal constraints on domestic intelligence collection and information gathering have been loosened the possibility of future terrorist attacks in the United States persists. These laws were changed to counter a newer, highly sophisticated terrorist threat that is no longer affiliated with a state actor whose main mission is the destruction of America and its citizens home or abroad. This coupled with the recognition that increased threats inside America originate from foreign entities and the rise of homegrown radicalism makes extending the law even more vital.

Allowing the provisions to sunset makes the government less intrusive and restores domestic intelligence collection to its pre 9/11 status. However, allowing the provisions to sunset will place strict limitations on domestic intelligence collection that could give terrorists the edge over early identification and prevention, exponentially increasing the risk to our nation.

The amount of time and evidence required to obtain approval to collect intelligence or gather information will be lengthened. Furthermore, the specific identification and location for each application will be required as opposed to a general search affording terrorists greater freedom of movement. Limiting the records that can

be obtained could create gaps in collection and allow terrorists to capitalize on technology and globalization to accomplish their aims.

Definitions, national guiding strategies, and the legislature are interwoven in the fabric of the domestic intelligence system. These elements coalesce within the organizations that comprise the whole of government and the domestic intelligence system responsible for safeguarding the nation. The next section describes and explains the links between the IC and HS, and the relationships between federal and state entities.

Organizational Structure

Existing organizational structures and systems facilitate the coordination and implementation of domestic intelligence policy and strategy. As noted, Congress mandated the establishment of the Department of Homeland Security and developed legislation to restructure the IC, in part, to resolve the information sharing dilemma within IC. It also sought to build stronger links between the IC, nontraditional federal, state, local, and Bureau of Indian Affairs/ tribal elements, as well as the public and private sectors to ensure catastrophic attacks against America do not happen again.

In general, the IC is a conglomeration of 16 executive agencies, departments, and military service organizations that work independently or together to perform intelligence activities to support foreign relations and to protect the national security of the United States.[35] Of the 16 organizations, four are considered nontraditional. They include the Drug Enforcement Agency's (DEA) Office of National Security Intelligence, Department of Energy's Office of Intelligence and Counter-Intelligence, Department of Homeland Security's Office of Intelligence and Analysis (I&A), and the Department of Treasury's Office of Intelligence and Analysis.[36]

Since congress defined homeland security information and redefined national intelligence or intelligence related to national security, all of these organizations now have a critical role in securing the homeland regardless of their roles prior to 9/11.

The Director of National Intelligence heads the intelligence community and oversees and directs the National Intelligence Program while serving as the principal advisor to the President. The Director's Office, ODNI, has several statutory components, but three directly link to homeland security.

The National Counterterrorism Center (NCTC) is responsible for the nation's counterterrorism intelligence analysis and counterterrorism strategic operational planning. It's Directorate of Information Sharing and Knowledge Development section ensures federal agencies have access to the information they need.[37]

Linked closely to the NCTC is the National Counterproliferation Center (NCPC). It provides a bridge between the IC and policy making elements within government. The NCPC also conducts strategic planning for the IC to support efforts to "prevent, halt, or mitigate the proliferation of WMD."[38]

The third key ODNI element linked to homeland security is the Program Manager of the Information Sharing Environment (PM-ISE). The Program Manager is responsible for planning, implementing, managing, and overseeing the ISE. The Program Manager's primary purpose is to enable information sharing and exchange of terrorism related information amongst the whole of government down to state, local and tribal governance.[39]

By its name, the Department of Homeland Security is the government's leading organization in unifying the national effort to protect the country against terrorist attacks

and responding to other threats and hazards.[40] The department's office of Intelligence and Analysis (I&A) "ensures that information related to homeland security threats is collected, analyzed, and disseminated to the full spectrum of homeland security customers in the Department, at state, local, and tribal levels, in the private sector, and in the IC."[41]

Additionally, the Under Secretary for Intelligence and Analysis, and Chief Intelligence Officer (CINT), oversees the department's internal Intelligence Enterprise (IE) responsible for integrating intelligence and information from the other DHS elements: Citizens and Immigration Services – Coast Guard – Customs and Border Protection - Immigration and Customs Enforcement - Transportation Security Administration. The Office of I&A also works to integrate intelligence/information from state, local, tribal, and private sector entities to fuse with intelligence from the IC, mainly the CIA, FBI, and NSA, to produce the most timely, accurate, and relevant products and warnings to prevent and disrupt attacks against America.[42]

Lastly, I&A serves as the executive agent for the department, state and local fusion center program while leading the DHS information sharing program.

73 state and regional Fusion Centers (FC) exist across the country. Congress defines Fusion Centers as "two or more Federal, state, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity."[43]

Fusion centers are not new, but took on added importance after 9/11. They are an outgrowth from former law enforcement centers and now consist of a multitude of

law enforcement and intelligence professionals, as well as first responders and other professionals as determined by state and local leaders.[44]

Fusion centers also provide the link between the states and federal government. Although there is no legally mandated model, DHS recognizes four "common and distinct functions" among fusion centers: they have information gathering requirements, they conduct some intelligence analysis and production, they facilitate information sharing and dissemination, and they possess prevention, protection, response, and recovery capabilities.[45]

Improvements and Challenges

The domestic intelligence system is improving. Several performance indicators suggest that significant improvements in the domestic intelligence system have been made since 2001. These examples represent only a few of these improvements.

First, improvements are being made in the integration of intelligence information between the CIA and the FBI. In January, 2009 the DNI announced the establishment of a web based database to be operational by the end of 2009 that will enable the FBI to access foreign intelligence in the same manner as other IC analysts. There are also discussions on setting a legal framework to enable the FBI to task foreign intelligence systems.[46] Additionally, with the help of former CIA analysts the FBI is making progress in training its analysts.[47]

Second, there is wide consensus among scholars, intelligence and law enforcement professionals, and think tanks such as Rand that significant advancements in information sharing have been made and are ongoing. The volume of information being passed between federal, state, local and tribal elements has increased exponentially and the number of systems and software architectures has proliferated

throughout the IC and domestic intelligence system. Between 2007 and 2009, for example, DHS disseminated 3,065 Homeland Intelligence Reports (HIR); DHS reported a 95% user rate of its Homeland Security Information Network (HSIN); and reported a 95% component-to component information sharing relationships documented through information sharing and access agreements.[48]

Third, DHS has taken measures to enhance internal systems to improve its intelligence cycle, improve intelligence/information sharing, and has reached out to states to improve fusion centers.

In an effort to become more efficient the DHS is currently undergoing a bottom up review to assess its overall structure, its systems, its tools, and its processes. Moreover, according to recent congressional testimony by the DHS Under Secretary for Intelligence and Analysis, the I&A office is realigning its operational element to better assist in its mission. The I&A office also intends to upgrade their operations section with new information technology to improve analysis, collaboration, and sharing between stakeholders.[49]

Additionally, by the end of 2009 the Office of I&A is expected to have 45 of its intelligence officers embedded in fusion centers throughout the country to better leverage capabilities in state and local areas, to assist in intelligence analysis and production, and to work with other stakeholders (DEA, FBI, ATF etc) to reduce redundancy and duplication of effort.[50] Lastly, not only will I&A work with and through fusion centers, it is endeavoring to do the same through the Interagency Threat Assessment and Coordination Group (ITACG).[51]

Nevertheless, even though great strides have been made to improve the security of the nation, many of these changes and improvements have created new problems or exacerbated existing ones. In spite of the 19 terrorist plots prevented and disrupted over the past nine years there is still much to be done to improve the domestic intelligence system. In general, the research indicates that the main challenges fall within three broad areas; organization, information sharing, and analysis.

The literature consistently cites three organizational problems; the impact of a decentralized domestic IC, continuing growing pains in the DHS, and long standing friction with the FBI.

At best, the 16 competing federal intelligence organizations, the numerous ancillary groups and private elements that feed the IC can be described as "complex and dispersed," or decentralized.

Critics argue that the IRTPA's objective of unifying the IC into an integrated enterprise with a shared mission and powerful CEO has not been realized.[52] As noted author James Lewis put it, "reorganization is not reform, although it can provide the means and opportunity for change."[53] Even though the DNI has more authority than the Director of the CIA, the DNI shares authority over the intelligence community with the Secretary of Defense, the Attorney General, and the Director of the FBI.[54]

The complicated relationship between states and the federal government presents further obstacles. Like DoD and DoJ, the DNI owns no portions of state, local and tribal enterprises and only has minimal influence over how their programs are run.[55] Moreover, even though states and localities are subject to the law, mayors do not work

for governors; and governors do not report directly to the President. Outside of the law there is no direct federal control built into the structure.

In 2009, Rand's Homeland Security Program and the Intelligence Policy Center released its report on *Reorganizing U.S. domestic Intelligence, Assessing the Options*. Because there was inadequate written information to assist in their assessment, Rand put together an expert panel composed of eight subject matter experts from across the whole of government, including intelligence professionals, policy makers, and practitioners.[56] The panel was critical of the "complex structure of the current domestic intelligence enterprise… [It] has no 'structure' and creates significant confusion for the domestic counterterrorism mission"[57] Additionally, when questioned about the effectiveness of the existing arrangements, panel members had mixed responses. They did, however, agree that redundancy among some departments and agencies results in "confusion and ambiguity about the roles of particular agencies with the domestic intelligence enterprise and uncertainty about who is responsible for what part of the effort."[58]

Other organizational dilemmas plague the DHS. There is overwhelming agreement on how much the DHS and it's I&A office has grown and improved, particularly in comparison to other IC organizations. Nevertheless, as in many larger organizations internal processes and procedures often impede effective and efficient internal synchronization and integration either horizontally or vertically.

In 2009, at the request of U.S. Representative Bennie G. Thomson, Chairman of the House Committee on Homeland Security, the DHS Inspector General (IG) reviewed information sharing processes within the DHS National Operations Center (NOC). The

DHS IG assessed whether procedures ensured that incoming reports were appropriately directed within the center; whether information was reviewed and disseminated in a timely manner to key department officials; and whether information was efficiently and effectively coordinated with other federal, state and local governmental partners.[59]

The IG's findings revealed that information sharing with the NOC is strained by administrative challenges. Stressed relationships between operations and intelligence personnel slowed the process. This was in part due to internal confusion over chain of command. "The Intelligence Side and the Operations Side have separate chains of command…Intelligence Side personnel report to the Under Secretary for I&A, while Operations Side personnel report to the Director of OPS."[60] This also resulted in intelligence personnel being unaware of their support role in the NOC, as well as their support role to the Senior Watch Officer and Assistant Senior Watch Officer (SWO/ASWO). Lack of appropriate intelligence support to the SWO/ASWO prevented them from adequately informing senior leaders in DHS creating potential vulnerabilities.

Compounding the problem was the lack of appropriately cleared personnel and a lack of understanding by NOC personnel of information security procedures; classification guidance, release authority, and procedures for handling sensitive information.[61] This also created unnecessary compartmentalization inside the NOC further exacerbating the problem.

The third key finding inside the NOC was a divide between intelligence and law enforcement personnel. This is related to the problem note above: law enforcement officers are not familiar with the proper procedures for handling classified information.

In the aftermath of the inspection, the IG learned this was a consequence of not understanding each other's roles, functions, and responsibilities.

The fourth finding was the lack of integrating intelligence personnel from other DHS components; Citizens and Immigration Services – Coast Guard – Customs and Border Protection - Immigration and Customs Enforcement - Transportation Security Administration. During the inspection only the Secret Service had an intelligence representative present in I&A.[62]

Even though no organization is perfectly efficient, these findings are antithetical to how good organizations operate. Unfortunately, it is in environments like this where critical pieces of intelligence/information get lost because of a lack of knowledge of what is being read or a lack of understanding of who needs to know and when they need to know it. Furthermore, this creates unnecessary gaps and vulnerabilities in the system, and places our adversaries in an advantageous position.

After a review of command and control issues within the homeland intelligence system and a review of internal DHS challenges the FBI is next. Of all the research there was overwhelming agreement on issues of concern for the FBI; specifically, cultural disorders, inability to adapt, and analysis and information systems concerns.

In her Intelligence and National Security Journal article, *9/11 and the FBI: The organizational roots of failure*, Professor Amy Zegart attributes the FBI's reticence to change as a result of "cultural pathologies"[63] and the subsequent inability to adapt to change. These pathologies originate with the establishment of the FBI and the image shaped by J. Edgar Hoover; "FBI agents as men of action…'G-men'…with an aversion to technology and analysis."[64] Throughout the Cold War the FBI was successful, but

the collapse of communism changed the paradigm and the FBI found itself outside of its "comfort zone" responsible not only for traditional law enforcement missions, but for preventing and disrupting asymmetrical threats against the U.S.[65]

Much has changed in the FBI, but its aversion to analysis and technology persists today. The relationship between Special Agents (SA) and intelligence analysts is indicative of the problem. Intelligence professionals are not afforded the same prestige as SAs. In fact, the three intelligence/counterintelligence divisions in the National Security Branch are lead by SA's as opposed to senior intelligence officers.[66] Their recruitment process also differs. Professor Hulnick further points out the "the Bureau's intelligence analysts are not 'first- class citizens;' only Special Agents hold that status…FBI analysts are hired in the same way as its truck drivers and other support people, where as in most IC organizations, analysts are as important as anyone else, and treated accordingly."[67]

The FBI's aversion to technology has also been a detriment to the Bureau impeding internal coordination. Prior to 9/11 the FBI operated and managed up to 42 antiquated systems with separate databases that were not interoperable. Consequently, they operated mainly on paper. After 9/11 the Bureau accelerated its implementation of their digital 'Trilogy' information system. The Trilogy information system was designed to upgrade the Bureau's computers, data network and servers, and provide investigative software.[68] It was also supposed to remedy the Bureau's information systems problems; but instead, according to Sen. Judd Gregg, Chairman of the subcommittee overseeing the Bureau's budget, "Trilogy has become a large disaster…the cost is soaring…the schedule is out of control."[69] The FBI also sought to

cut back on Trilogy funding to offset budget cuts. This resulted in a negative backlash from Congress. In response, for example, Sen. Charles E Schumer remarked, "the FBI continues to operate with a 20th century computer system as terrorists are engaging in 21st century cyber warfare."[70]

In a more recent example, November 2008, the DoJ IG found that the FBI's Guardian system, which stores terrorist reporting and information, possessed numerous "data integrity failures, including failures of supervisors to conduct a review to determine whether a threat was adequately addressed, and failure to create a complete record for fully 30% of examined records."[71]

The next sets of obstacles within the domestic intelligence system are inside the Information sharing domain. In their earlier mentioned 2009 report, Rand, like many others, acknowledged the improvements in information sharing. However, Rand's expert panel expressed concern whether the IRTPA and IC's transformation in organization and information will "yield enduring institutional change required to address our current threat environment."[72] In the same report, the panel questioned, as did the 2005 WMD commission, "whether transferring information by sharing personnel among agencies or in multi-agency centers is enough to provide all agencies' analysts sufficient access to other organization's intelligence information for effective analysis."[73] Unfortunately, the well publicized Christmas day, 2009 attempted terrorist attack on flight 253 by Nigerian national Umar Farouk Abdulmutallab validated Rand's above concern.

As was the case with the other issues discussed above, the preponderance of research points to three factors that continue to impede timely and efficient information

sharing; the volume and types of reports, systems-architectures-networks and, personnel and information security. Because the federal government and states have different priorities and intelligence requirements, knowing what to report is often confusing and makes this endeavor even more complicated.

Processing and analyzing reports and information that enters the intelligence stream from 16 departments/agencies, state – local – tribal elements, as well as intelligence from other nations is a daunting task. The FBI's E-Guardian information sharing enterprise for example facilitates the exchange of information across 18,000 entities.[74] Moreover, between 2004 and 2007, "the FBI documented 108,000 potential terrorism-related threat reports of suspicious incidents, and terrorist watchlist encounters."[75] This represents only one agency and is a fraction of what the IC processes' and analyzes.

9/11 and the changing international environment with hybrid asymmetric threats makes preventing and disrupting the next attack on the homeland extremely complicated. Consequently, we are now in an era where many argue there are too many dots to connect and that our systems are flooded with information that often lacks quality or is redundant.

Not knowing what to report and the amount of reporting can overwhelm the system slowing and clogging it. The volume and quality of reports can rapidly exceed the number of available analysts and their capability to process and or extrapolate the meaning of what they read. As the Rand study found, there was a "lack of coordination in domestic collection efforts, and volume of data of questionable or poorly specified quality."[76] Moreover, a 2007 GAO report found this to be true as well when "identical or

similar types of information are collected by or submitted to multiple agencies, integrating or sharing this information can lead to redundancies…in fusion centers, multiple information systems created redundancies of information that made it difficult to discern what was relevant. As a result, end users were overwhelmed with duplicative information from multiple sources."[77] Similar results continued in a later GAO report in 2008. Here, the GAO found that half of the fusion centers they contacted reported "they had...challenges in accessing federal information systems, while at the same time over half reported that the heavy volume of information they were receiving and the existence of multiple systems with redundant information were difficult to manage."[78]

Noted earlier, the number of information systems, their data bases, and their lack of interoperability further inhibits the information sharing process of getting the right intelligence/information to right person or agency at the right time. In the CRS' 2009 report on *Terrorism Information Sharing and the Nationwide Suspicious Reporting Initiative: Background and Issues for Congress*, "there are currently in place or under development, 266 separate systems that share information about crime, including terrorism, at the national, regional, sate levels."[79] The report further observes that the proliferation of systems "has lead to a concern that it is hard to know what information is being shared and who is sharing it. In many cases, multiple systems are being developed to cover overlapping areas."[80]

In addition to the 266 separate systems, the NCTC (nexus of all things terrorism) accesses approximately 30 intelligence, law enforcement, and military networks to obtain intelligence information.[81] Classification restrictions on information and networks require NCTC analysts to use three separate computers on their desks to access data.[82]

The NCTC is in the process of standing up an Information Sharing Enterprise designed to address these challenges; however, it is not known if their new system is fully operational.

Like the states and the NCTC, the DHS is not without its trials. In its haste to put into operation its Homeland Security Information Network (HSIN) the department took short cuts to make it operational. The department failed to reconcile collaborative systems and tools, and did not "obtain address requirements from all HSIN user communities in developing the system…the department has not provided adequate user guidance, including clear information sharing processes, training and references materials."[83]

These short cuts prevent the system from realizing its intended potential and do a disservice to the consumers while placing the country at greater risk. It further results in a lack of confidence in the system perpetuating bad habits or resorting to old ways which contributed to 9/11. Similar observations were cited in a 2006 DHS IG report, "HSIN is not effectively supporting state and local information sharing...users are confused and frustrated, without clear guidance on HSIN's role or how to use the system's ability to share information effectively…because the system does not provide them with useful situational awareness and classified information, users do not regularly use HSIN."[84] In fairness to DHS, they did later report a 95% component-to component information sharing relationship documented through information sharing and access agreements on its HSIN. However, it is not known if DHS corrected the deficiencies noted in their earlier IG report or whether the system is meeting its full potential.

The next obstacle to the timely and effective flow of intelligence/information is security clearances and the nature of classified information. This amplifies earlier discussions. In report after report practitioners and professionals like Rand, Oracle, Professors Hulnick and Zegart, to name a few, vehemently argue that security clearances, classified information and its associated guidance, as well as operating systems and networks can bring the sharing enterprise to its knees.

Common examples include over classifying information, or not knowing what to classify based on sources. Oracle, for instance, found that in fusion centers many agencies and departments had separate classified systems that only their personnel were authorized to use.[85] Having representatives co-located in one location below the federal level is a positive action that creates a vital synergy with intelligence reporting and analysis. However, limited access and stovepipe systems are the antithesis of fusion and increases risk by creating multiple points of failure in the domestic intelligence system.

Further frustrating the process is the divide between the federal IC, state-local-tribal law enforcement and intelligence entities and private sector security procedures. Each entity has its own system. The federal government classifies information as Top Secret/Secret/Confidential/For Official Use Only (also Sensitive but Unclassified (SBU)with caveats depending on the type of source. Law enforcement on the other hand, has its own system and uses such classifications as Law Enforcement Sensitive (LES). At the same time the private sector has a separate industry standard. Therefore, when reporting or viewing intelligence/information who decides what information gets fed into the system and by what standard of classification or

declassification? Additionally, once information is in the system who decides who else needs to know and what they need to know, and through what means or systems do they communicate the info? These questions are indicative of the existing friction in the system today.

Classified networks and domains commensurate to the classification of the information they pass further compounds the problem. The location, or domain where the information resides makes matters worse; .gov, .mil, service domains, and agency domains do not permit intelligence/information to pass between domains, vertically or horizontally. If an analyst, like the NCTC, needs access to a particular report on not on one of their system the analysts uses work arounds to gain access to the report, thus slowing the process.

The third and last ongoing broad concern within the domestic intelligence system is intelligence analysis. Like personnel and information security, intelligence analysis along with quality, training, and Human Resources (HR) were prevailing themes throughout the literature.

The 9/11 Commission report concluded "a 'smart' government would integrate all sources of information to see the enemy as a whole."[86] Similarly, many now recognize that information obtained for one purpose could provide special meaning when compared and merged with other unrelated sources of information. The Markle Foundation says it best, "relevant information comes from a much wider range of sources…and it is difficult to know *a priori* what information will prove relevant to analysts or useful to users… there is an especially critical need to allow [for] the analysis and connect them to users in [or] at the international, federal, state, and local

levels, as well as to the private sector."[87] The report goes on to say that "because this form of analysis is heavily dependent on large volumes of data (to detect patterns and to make correlations) assuring the quality of data is critical."[88]

The sources and volume of intelligence and information, as well as the size of the domestic intelligence enterprise have grown exponentially. This has had a blunting impact on our nation's ability to "connect the dots" to remain ahead of our adversaries. In essence, it is a race against time to ensure that there is a professional force of adequately trained analysts throughout the whole of government to ensure that timely, accurate, and relevant intelligence/information is at the right place and time to prevent future attacks on the homeland. Unfortunately, this is not always the case. Rand and CSIS' James Lewis, as well as scholars site the opposite. Rand for example, identified four systemic problem areas: "a lack of appropriately skilled and trained analysts/staff; a law enforcement culture that discounts exploratory analysis; fragmented, uncoordinated competing and conflicting analysis that clogs the system; and insufficient analytic techniques and data to effectively identify as-yet-unknown domestic threats."[89]

Contributing to this dilemma is sub optimal recruiting and training. Building a quality force begins at the initial entry point of any organization followed by sound training and a professional education system. Hulnick and others say this is not so within the domestic intelligence system. He opines that many organizations, excluding the military, have fragmented systems.

In contrast to maintaining an enduring professional recruiting force the CIA, for instance, sends out officers from within its different directorates and its intelligence officers on rotational assignment to recruiting duty. Furthermore, the rest of the IC,

Hulnick points out, “don’t even bother, but take whatever emerges from the recruitment Website.”[90]

Conclusion

Once the IC organizations, bureaucracy, systems and tool are established the domestic intelligence system and enterprise should not remain static. Rather, like Joint Intelligence Preparation of the Environment (JPIOE) and Intelligence Preparation of the Battlefield (IPB) the domestic intelligence system/enterprise must remain dynamic and ever changing to keep ahead of adaptive and evolving threats.

The research in this project showed that emerging and adaptive threats, including an increase in domestic (homegrown) radicalization, requires us to constantly evaluate the boundaries between foreign, domestic, and law enforcement department/agencies, their roles and responsibilities, and the applicable laws that that allow them to operate. Furthermore, the nature of the today’s threats in America means that all sectors of society take on greater roles in identifying and preventing future attacks on the homeland.

The data overwhelming supports the supposition that the domestic intelligence system is moving in the right direction. “Walls” between the FBI, CIA, and NSA are being chipped away, structures have been changed or newly created to address shortfalls after 9/11, and laws have been amended to allow our intelligence and law enforcement operations keep pace with globalization and improved technologies our adversaries use to attack us.

Be that as it may, the whole of government, the Intelligence and law enforcement communities, practitioners, and scholars agree that our domestic intelligence system still faces many problems. Our domestic intelligence system is not complete.

The decentralized nature of the domestic intelligence system, coupled with internal strife in the DHS, and the FBI's slowness in balancing foreign over domestic intelligence analysis and technologies continue to plague the system.

Information sharing is not as responsive at it should be. The system has not kept pace with the increase in volume of traffic/reporting. The different security classification levels and systems with the current security clearance policy and process severely encumber the information sharing system. Together, with databases and networks that are not interoperable and the flooding of intelligence/information processors further impedes the intelligence and law enforcement communities progress in information sharing (processing, analysis, and dissemination).

Lastly, there are not enough intelligence analysts commensurate with the increase in organizational demand, and the volume and diversity of reporting. Coupled with inadequate recruiting practices and decentralized training, intelligence analysis is sub-standard creating wider gaps in intelligence cycle and the nation's indications and warning system.

Endnotes

[1] In fatwa entitled Jihad against Jews and Crusaders World Islamic Front statement, 28 Feb 98.

[2] George W. Bush, *National Strategy for Homeland Security* (Washington, DC: The White House, October 2007), 3.

[3] Arthur S. Hulnick, "Intelligence Reform 2008: Where to from Here?" *International Journal of Intelligence and counterintelligence* 21, no 4 (2008): 628.

[4] U.S. Department of Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington DC: U.S. Department of Defense Joint Staff, 12 April 2001, As Amended Through 19 August 2009), 269.

[5] Mark A. Randol, Mark A., "Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches," *Congressional Research Service*, (January 14, 2009), RL33616, 9.

[6] Randol, 11.

[7] Barack H. Obama, *The National Intelligence Strategy of the United States of America* (Washington, DC: The House August 2009), 6.

[8] National Intelligence Strategy (NIS), Forward.

[9] National Strategy for Homeland Security Strategy (NSHS), 1.

[10]NIS, 6.

[11] NSHS, 1.

[12] NIS, 12.

[13] Ibid., 12.

[14] NSHS, 4.

[15] Ibid., 4.

[16] NIS, 14.

[17] NSHS, 49.

[18] Roger Z. George and Robert D. Kline, eds., *Intelligence and the National Security Strategist: Enduring Issues and Challenges* (Washington DC: Sherman Kent Center for Intelligence Studies, National War College, National Defense University Press, 2004), 63.

[19] Edward C. Liu, "Amendments to the Foreign intelligence Surveillance Act Set to Expire in 2009," *Congressional Research Service*, (March 14, 2009), R40138, 2.

[20] Ibid., Summary.

[21] Ibid., 2

[22] Information on Zacarias Moussaoui is well documented in multiple sources.

[23] Liu, 3.

[24] Ibid., 3.

[25] Ibid., 2.

[26] Ibid., 4.

[27] Ibid., 5.

[28] Ibid.

[29] Ibid., 8.

[30] Ibid., 9.

[31] Ibid.

[32] Ibid., 10.

[33] Ibid., 5.

[34] U.S. Congress. House. 2009, *Department of Defense Appropriations Act, 2010*, HR 3326. 11th Con., 1st sess., 62.

[35] U.S. Office of the Director of National Intelligence, "2009, National Intelligence A Consumer's Guide," (Washington DC: U.S. Office of the Director of National Intelligence, 2009), 7.

[36] The four nontraditional departments and agencies are based on the assumption that the other 12 departments and agencies are common knowledge amongst the field.

[37] National Intelligence Consumers Guide, 24.

[38] Ibid., 26.

[39] Ibid., 31.

[40] Ibid., 48.

[41] *U.S. Department of Homeland Security, Office of Intelligence and Analysis Home Page*, http://www.dhs.gov/xabout/structure/gc

[42] Ibid.

[43] Mark A. Randol, Mark A., "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress," *Congressional Research Service*, (May 27, 2009), R40602, 14.

[44] John Rollins, "Fusion Center: Issues and Options for Congress, Congressional Research Report for Congress," *Congressional Research Service*, (January 18, 2008), RL34070, 1.

[45] Ibid.

[46] Arthur R. Hulnick, "Home Time: A New Paradigm for Domestic Intelligence," *International Journal of Intelligence and counterintelligence* 18, no 3 (2009): 580.

[47] Ibid., 581.

[48] U.S. Department of Homeland Security, *Strategic Plan, Fiscal Years 2008-20013, One Team, One Mission, Securing Our Homeland* (Washington DC: U.S. Department of Homeland

Security), 22-25. Note also, the Fiscal Years 2007-2009 APR provides the mission oriented programs and performance measures according to the objective structure that was in place during FY 2007.

[49] Bart R. Johnson, Acting Under Secretary for Intelligence and Analysis Before the Subcommittee n Intelligence, Information Sharing, Terrorism Risk Assessment on "I&A Reconceived: Defining Homeland Security Intelligence Role", *US Fed New Service, Including US State News*, (September 25, 2009).

[50] Bart R. Johnson, Acting Under Secretary for Intelligence and Analysis Before the Subcommittee on Intelligence, Information Sharing, Terrorism Risk Assessment on "Fiscal Year 2010 Budget Request," *US Fed New Service, Including US State News*, (June 25, 2009).

[51] Ibid., 6. The President and Congress directed establishment of the ITACG to improve the sharing of information with State, local, tribal, and private sector (SLTP) officials within the scope of the Information Sharing Environment (ISE). The ITACG supports the efforts of the National Counterterrorism Center (NCTC) to produce "federally coordinated" terrorism-related information products intended for dissemination to State, local, and tribal officials and private sector partners through existing channels established by Federal departments and agencies

[52] James Lewis, *Section 4, Intelligence*; James A. Lewis is a senior fellow at CSIS and directs its Technology and Public Policy Program. His research involves innovation and economic change; Internet policy and cyber security; space programs; and intelligence reform.

[53] Ibid.

[54] Ibid.

[55] Hulnick, "Home Time," 577.

[56] Gregory F. Treverton, "Reorganizing U.S. Domestic Intelligence, Assessing the Options," *Rand Homeland Security Program and the Intelligence Policy Center* (2009): 25.

[57] Ibid., 26.

[58] Ibid.

[59] Department of Homeland Security, Office of the inspector General, *Informational Sharing at the National Operations Center (Redacted)*, (Washington DC: Department of Homeland Security, Office of the Inspector General, November 2009), OIG-10-15, 1.

[60] Ibid., 23.

[61] Ibid., 24.

[62] Ibid., 45.

[63] Amy Zegart, "9/11 and the FBI: The organizational roots of failure," *Intelligence and National Security* 22, iss. 2, (April 2007): 164-184.

[64] Ibid., 3.

[65] Ibid.

[66] Hulnick, “Intelligence Reform,” 628.

[67] Ibid.

[68] Donald F. Kettl, “Reshaping the Bureaucracy,” in *System Under Stress: Homeland Security and American Politics,* 2d edition. (Washington, DC: CQ Press, 2007), 44-45.

[69] Ibid., 45.

[70] Ibid.

[71] Gregory T. Nojeim, Director Project of Freedom, Security & Technology, Before the House Homeland Security Committee Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, “Homeland Security Intelligence: Its Relevance and Limitations,” *Center for Democracy & Technology*, (March 18, 2009), 8.

[72] Treverton, “Reorganizing U.S.,” 35-35.

[73] Ibid., 35.

[74] Nojeim, Center for Democracy & Technology, pg 7.

[75] Mark A. Randol, “Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress,” *Congressional Research Service*, (November 5, 2009), R40901, 16.

[76] Treverton, “Reorganizing U.S.,” 30-31.

[77] Randol, “Terrorism Information Sharing,” 15-16.

[78] Nojeim, “Homeland Security,” 8.

[79] Randol, CRS, pg 4.

[80] Ibid., 4.

[81] Nojeim, “Homeland Security,” 7.

[82] Helen Fessenden, “The Limits of Intelligence Reform,” *Foreign Affairs* 84, (Nov/Dec 2005): 8.

[83] Department of Homeland Security, Office of the inspector General, *Homeland Security Information Network Could Support Information Sharing More Effectively*, (Washington DC: Department of Homeland Security, Office of the Inspector General, November 2006), OIG-06-38, 3-4.

[84] Ibid., 4.

[85] Chuck Dodson, “Use of Technology in Intelligence Fusion Centers, An Oracle White Paper April 2007,” *Oracle*, (April 2007): 6.

[86] “The 9/11 Commission Report,” 401.

[87] “Protecting Freedom in the Information Age, a Report of the Markle Foundation Task Force,” *The Markle Foundation*, (October 2002): 48.

[88] Ibid., 48.

[89] Treverton, “Reorganizing U.S.,” 31-34.

[90] Hulnick, “Intelligence Reform,” 629.